CSC-EPL-88/004


NATIONAL COMPUTER SECURITY CENTER



# FINAL EVALUATION REPORT OF SPECTRUM MFG. INC.

# DATA PROTECTION SYSTEM

# 800/12



2 May 1988

# REPORT DOCUMENTATION PAGE

| | |
|---|---|
| 1a. REPORT SECURITY CLASSIFICATION<br>UNCLASSIFIED | 1b. RESTRICTIVE MARKINGS<br>None |
| 2a. SECURITY CLASSIFICATION AUTHORITY | 3. DISTRIBUTION/AVAILABILITY OF REPORT<br>Approved for public release;<br>Distribution Unlimited |
| 2b. DECLASSIFICATION/DOWNGRADING SCHEDULE | |
| 4. PERFORMING ORGANIZATION REPORT NUMBER(S)<br>CSC-EPL-88/004 | 5. MONITORING ORGANIZATION REPORT NUMBER(S)<br>S230,628 |
| 6a. NAME OF PERFORMING ORGANIZATION<br>National Computer Security Center<br>6b. OFFICE SYMBOL (If applicable) C12 | 7a. NAME OF MONITORING ORGANIZATION |
| 6c. ADDRESS (City, State and ZIP Code)<br>9800 Savage Road<br>Ft. George G. Meade, MD 20755-6000 | 7b. ADDRESS (City, State and ZIP Code) |
| 8a. NAME OF FUNDING/SPONSORING ORGANIZATION<br>8b. OFFICE SYMBOL (If applicable) | 9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER |
| 8c. ADDRESS (City, State and ZIP Code) | 10. SOURCE OF FUNDING NOS<br>PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT NO |
| 11. TITLE (Include Security Classification)<br>(U) Subsystem Eval Report - Spectrum Mfg., Inc., DPS-800/12 | |
| 12. PERSONAL AUTHOR(S)<br>Schneider, Stephen; Crescenzi, Caralyn; Oehler, Michael; Wyszynski, John | |
| 13a. TYPE OF REPORT<br>Final<br>13b. TIME COVERED FROM TO | 14. DATE OF REPORT (Yr, Mo., Day)<br>880502<br>15. PAGE COUNT<br>20 |
| 16. SUPPLEMENTARY NOTATION | |
| 17. COSATI CODES<br>FIELD / GROUP / SUB. GR. | 18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)<br>NCSC; TCSEC; I&A; Spectrum Mfg.; test and evaluation; identification authentication; DPS-800/12; (KT) |

19. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The Data Protection System-800/12 (DPS-800/12) is a dial-up security device that provides identification and authentication for a host system. The DPS-800/12 consists of a Controller Card, an optional Printer/Log Card, and from one to twelve Port Cards. The Controller Card uses a microprocessor and contains the DPS-800/12 system program. This card controls the Printer/Log Card and the Port Cards. The Printer/Log Card drives the printer in order to print the audit records. Each Port Card controls a communication line between a modem and the respective host. This report documents the findings of the evaluation. (computer security; computer software;)

| | |
|---|---|
| 20. DISTRIBUTION/AVAILABILITY OF ABSTRACT<br>UNCLASSIFIED/UNLIMITED | 21. ABSTRACT SECURITY CLASSIFICATION<br>UNCLASSIFIED |
| 22a. NAME OF RESPONSIBLE INDIVIDUAL<br>DENNIS E. SIRBAUGH | 22b. TELEPHONE NUMBER (Include Area Code) (301)859-4458<br>22c. OFFICE SYMBOL C/C12 |

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

# SUBSYSTEM EVALUATION REPORT

# SPECTRUM MFG., INC.

# DATA PROTECTION SYSTEM-800/12

NATIONAL
COMPUTER SECURITY CENTER

9800 SAVAGE ROAD
FORT GEORGE G. MEADE MARYLAND
20755-6000

May 2, 1988

CSC-EPL-88/004
Library No. S230,628

This page intentionally left blank

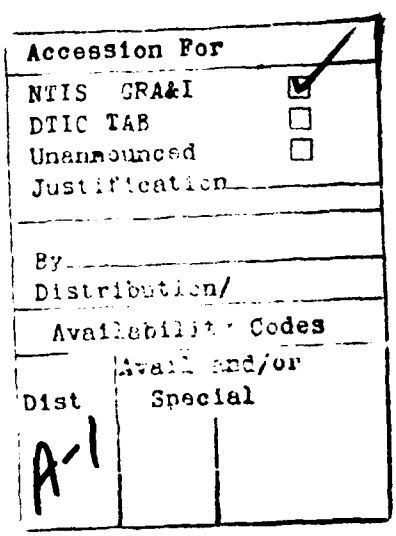
## Foreword

This publication, the Subsystem Evaluation Report of Data Protection System-800/12 made by Spectrum mfg., inc., is issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." This report documents the results of an evaluation of Spectrum's Data Protection System-800/12 product. The requirements stated in this report are taken from *Department of Defense Trusted Computer System Evaluation Criteria* dated December 1985.

Approved:

Eliot Sohmer May 2, 1988

Eliot Sohmer
Chief, Computer Security Evaluations,
Publications, and Support
National Computer Security Center

## Acknowledgements

Evaluation Team Members

Stephen D. Schneider

Caralyn A. Crescenzi

Michael J. Oehler

John L. Wyszynski

National Computer Security Center
9800 Savage Road
Fort George G. Meade, Maryland
20755-6000

## Table Of Contents


Foreword ..... iii
Acknowledgements ..... iv
Executive Summary ..... vii

Section 1 Introduction ..... 1
- Background ..... 1
- The NCSC Computer Security Sub-system Evaluation Program ..... 1

Section 2 Product Evaluation ..... 3
- Product Overview ..... 3
- Evaluation of Functionality ..... 3
  - Physical System Setup ..... 3
  - Identification & Authentication ..... 4
  - Audit ..... 5
- Evaluation of Documentation ..... 6
  - DPS-800/12 Operator Manual ..... 6
  - Audit Report Generator ..... 7
  - Audit Report Generator Runbook ..... 8

Section 3 The Product In A Trusted Environment ..... 9

Section 4 Product Testing ..... 11
- Test Procedure ..... 11
- Test Results ..... 11

This page intentionally left blank

## Executive Summary

The Data Protection System-800/12 (DPS-800/12) is a communication port protector which has been evaluated by the National Computer Security Center (NCSC). The DPS-800/12 is considered to be a sub-system rather than a complete trusted computer system; therefore, it was evaluated against a relevant subset of the requirements from the *Department of Defense Trusted Computer System Evaluation Criteria* (Criteria). The subset of the Criteria that applies to DPS-800/12 included Identification & Authentication (I & A) and Audit.

The DPS-800/12 is available in both synchronous and asynchronous modes which are addressed in the following paragraphs:

The DPS-800/12 has a synchronous mode of operation which was not tested since the Operator's Manual stated that in this mode the requirement for a user supplied password is bypassed. This fails to meet the requirement for a user to identify himself by an explicit action. Therefore, the synchronous mode does not satisfy the minimum requirements of the Criteria for Identification and Authentication and was not considered part of the evaluation.

However, the DPS-800/12 provides some security functionality when operating in the asynchronous mode. In this mode, it was determined that a user is able to access the host system only after entering a valid password. The system administrator is responsible for assigning passwords which will enforce unique identification of users.

The NCSC evaluation team has determined that the asynchronous product functioned as claimed, but the lack of precise documentation may lead to its improper management. If the system administrator is able to understand the principle and operation of the product, then the security administrator could install the DPS to provide additional security features. Therefore, there may be limited applications in which an asynchronous DPS-800/12 could provide a level of protection to satisfy the needs of a particular environment.

This page intentionally left blank

# Introduction

## Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all federal government agencies. As a result, the Center became known as the National Computer Security Center (NCSC) in August 1985.

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems. Trusted computer systems are those that employ a sufficient number of hardware and software integrity measures in the processing of a range of sensitive or classified information. Such encouragement is brought about by first evaluating and publishing the technical protection capabilities of existing systems (whether developed by industry or government.) Also productive is the advising of system developers and managers of their systems' suitability for use in processing sensitive information. Finally, significant encouragement will be achieved by assisting in the incorporation of computer security requirements in the systems acquisition process.

## The NCSC Computer Security Sub-system Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Sub-system Evaluation Program.

The goal of the NCSC's Computer Security Sub-system Evaluation Program is to provide computer installation managers with information on sub-systems that would be helpful in providing immediate computer security improvements to existing installations.

Sub-systems considered in the program are special-purpose products that can be added to existing computer systems to enhance some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security sub-system evaluation is limited to consideration of the sub-system itself, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations an attempt is made, where appropriate, to assess a sub-system's security-relevant performance in light of applicable standards and features outlined in the Criteria.

Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be placed on the Evaluated Products List.

The report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

## Product Evaluation

### Product Overview

The Data Protection System-800/12 (DPS-800/12) is a dial-up security device that provides identification and authentication for a host system. The DPS-800/12 consists of a Controller Card, an optional Printer/Log Card, and from one to twelve Port Cards. The Controller Card uses a microprocessor and contains the DPS-800/12 system program. This card controls the Printer/Log Card and the Port Cards. The Printer/Log Card drives the printer in order to print the audit records. Each Port Card controls a communication line between a modem and the respective host.

The DPS-800/12 uses an optional hardware device, the User Verifier (UV-1) which provides the added security feature of identification. Although this device is optional, it is considered vital for security operations and is thus a part of the evaluated configuration. The UV-1 connects to the system between the remote terminal and remote modem. The system administrator may specify whether each user is required to have a UV-1 to gain access to the system. If the user requires a UV-1, the DPS-800/12 sends a signal to the UV-1 requesting its unique identifier. When the DPS-800/12 receives the correct identifier, the individual may access the system. If a UV-1 is not required, the individual may gain access through the DPS-800/12 by simply entering a password.

This system provides mechanisms by which the system administrator can limit users to specified ports as well as specified access time slots. For example, a user might be able to gain access on only two ports between 8 AM and 5 PM daily. Each port is associated with one modem connection.

The system may operate in either a synchronous or asynchronous mode. In the synchronous mode, the remote user only needs an authorized UV-1 unit; so, this mode eliminates the entering of a password. In the asynchronous mode, the user must enter a password in addition to using the UV-1, before accessing the system. Since the synchronous mode does not provide authentication, the DPS-800/12 was tested only in the asynchronous mode.

### Evaluation of Functionality

#### Physical System Setup

The DPS-800/12 is installed between the host system and its dial up modems, using the standard RS-232C protocol as the interfaces. More specifically, each port card is connected between the host and a modem. Only the system administrator console, not the main host system, can be used to control the security functions of the DPS-800/12. This console has its own port on the back of the

DPS-800/12 through which it controls all accesses and privileges associated with this system. The advantage of this configuration is that users with access through the DPS-800/12 are unable to compromise the security of the system by changing its security functions. Physical access and knowledge of the administrator's password is required to make additions or deletions from the password lists or to use any of the other security functions.

An alternate option allows the system administrator to configure the DPS-800/12 to grant users access to the host system without the UV-1. Exercising this option retains the time-of-use and port restriction features of the system but obviously loses some assurance gained through the use of UV-1's.

The UV-1's are distributed to users with remote terminals and modems, and are intended to be connected between them. Again the standard RS-232C protocol is used as the interface. Because of the requirement to cable the UV-1 into the user's system, Spectrum's system is not very portable. Due to this relative lack of portability, a user who leaves a UV-1 in an unsecure area loses a degree of assurance. However, when a UV-1 is permanently installed in a physically secure area, the degree of assurance increases.

Identification & Authentication

(Asynchronous Mode)

With a UV-1 installed, proper access to the host system is gained by dialing the host, entering a password, and waiting for a signal from the DPS-800/12 to continue with the standard log on procedure for the host system. Specifically, access is granted in the following manner:

> A dial up connection is made to the host system's modem. After this connection is made, the DPS-800/12 port card waits without providing a prompt for the user to enter a recognizable password, which begins with the attention character. When this is complete, the port card signals the DPS-800/12 controller to check the incoming string of characters against its internal password list.
>
> Unlisted passwords are audited and displayed on the connected audit device, (i.e. printer or terminal). If the password is listed, then the time of call and accessed port is compared against his time slot and port group lists. If the system administrator has placed the same password in the database of valid users more than once, only the first occurrence will be checked for verification.
>
> If the password is authorized, a random control sequence is sent back to the remote user. This control sequence will appear on the screen of a user without a UV-1 as

random characters. However, if a UV-1 is attached, it will capture the sequence and process it internally. The UV-1 generates a new sequence based on the incoming sequence, the system internal key, and the UV-1 serial number. The UV-1 sends this new sequence back to the DPS-800/12 which compares it to its pre-determined response.

Once the DPS-800/12 recognizes the proper UV-1 response, the DPS-800/12 relinquishes control and notifies the remote user, by sending the word "continue". This indicates that the connection to the host system has occurred. At this point, the host's own log on sequence may be issued.

After the connection is complete, the UV-1 has no other function other than passing data between the remote terminal and its modem. Although the UV-1 is still hooked up, it can be powered down. It can even be removed although this may jeopardize the telephone's connection.

Unlike the UV-1, the DPS-800/12 must remain powered on. It is responsible for handling incoming calls, audit data, system administrator access, and port de-activation. The DPS-800/12 is also responsible for passing data between the host and its modems.

The port cards monitor connections, waiting for log off sequences. This sequence of characters must exactly match the pre-defined log off sequence and occur only immediately after a carriage return. After a user enters the sequence, the DPS-800/12 will de-activate the accessed port. The accessed port will also be de-activated through the negation of the modem's DSR line. This occurs when the phone line is hung up. Further communication to the host would then require another connection, as previously described.

Audit

The DPS-800/12 maintains a chronological audit trail on a serial device connected to the audit port of the DPS-800/12. The DPS-800/12 records illegal password attempts, dial-up timeouts, incorrect UV-1 responses, accesses to the DPS-800/12's data base, and found UV-1's.

Even though the DPS-800/12 controller maintains an audit trail and provides several audit features, care must be used in the implementation of this feature. The audit trail is based on the UV-1 serial numbers, not on the user's identity. As a result, if the system administrator allows more than one individual to use the same UV-1, individual auditing may become difficult.

## Evaluation of Documentation

The DPS-800/12 documentation consists of three documents: the *Operator Manual*, the *Audit Report Generator,* and the *Audit Report Generator Runbook.* Since the audit software package was not provided during this evaluation, the audit documentation was not assessed for correctness. In addition, a document for users was not available and therefore, users should rely upon documentation from the security administrator or their instructions.

## DPS-800/12 Operator Manual

This forty-eight page document contains a general introduction to the DPS-800/12 system and instructions for its overall use. This manual is intended for an individual who installs and/or administrates the system. The administrator uses this manual to learn the functions and privileges that should be controlled. In the process of testing the system and verifying the documentation, the team observed several problem areas, in addition to the poor organization of the document.

Although it doesn't, the documentation should state that the system administrator should assign only unique passwords (including unique time slots and port groups) for individuals using the same UV-1. Otherwise, the system administrator may not be able to determine which user accessed the system.

Throughout this document, terminology is inconsistently used. For example, password, password number, number, serialized UV-1 number, UV-1 serial number, and system identifier are occasionally used interchangeably. This makes the document difficult to understand.

The description of the "lost UV-1 option" is unclear and misleading. The manual states that a lost UV-1 may be deleted from the "lost" list. This implies that the UV-1 may be returned to function correctly. In fact, testing illustrated that the lost UV-1's system identifier is changed. This means that the UV-1 cannot regain access even though it has been found unless an "UV-1 programmer" is purchased and used. This requirement was not mentioned in any documentation.

### Chapter 1: Introduction

The first section provides a brief description of the DPS-800/12 system's configuration and use. The chapter also contains sections on the following: Auto Log On, User Verifier, Printer/Log Controller, and Specifications. The Auto Log On section is incomplete and only the UV-1 unit attributes are mentioned. These comments could be contained more appropriately in the User Verifier section.

Chapter 2: Operation

This chapter describes how the cards (also called modules) perform and interact with each other. The second section explains what each LED indicates.

Chapter 3: Installation

This section explains how to install the DPS-800/12. Step-by-step instructions explain system installation, and a front view diagram aids in illustrating the card positions. This section states falsely that a UV-1 is required. However, this is not always true, as noted in the functionality section of this report.

Chapter 4: System Set-up

This chapter provides system configuration information. Step-by-step instructions show how to configure the DPS-800/12 with an asynchronous terminal. A table of main menu commands lists a brief description of each and refers to sections for more detail. This is incomplete, because it does not contain all of the menu options; port options and log off are not documented. In addition, this section needs to explain how to configure the modem into the system.

Appendices A and B

In Appendix A the internal diagnostics, network diagnostics and report formats are explained. Appendix B provides a description of the auto log on feature for the asynchronous mode as well as the synchronous mode. Testing illustrated that the description of the asynchronous mode is incorrect because the "security check" prompt is not displayed as stated.

NOTE: The following documents were not tested for correctness; therefore only the contents of the documents are described.

Audit Report Generator

This four page document briefly describes Spectrum's Audit Reporting Package. This software package is used with an IBM PC or BIOS compatible computers. The document contains a short explanation of the audit data and system configuration. In addition, Spectrum describes each choice of the main menu and states that a detailed instruction manual, the Audit Report Generator Runbook, may be purchased separately.

Audit Report Generator Runbook

This document provides a detailed description of the Audit Reporting Package. The manual contains a system overview and explains the installation of the Audit Package, a menu driven program. Certain sections of the manual briefly describe each menu option.

## The Product in a Trusted Environment

The DPS-800/12 can be used, as-is from the manufacturer, to add security to virtually any computer system that uses standard RS-232C communication protocol on its dial-up lines. The data terminal ready (DTR) signal must operate according to the RS-232C standard for proper operation of the system. This is necessary for connections to be recognized.

When installed, as tested, the DPS-800/12 will monitor and control all accesses made through it to the host system. It will produce an audit log of all attempts made; however, they are immediately transmitted to an external audit collection device (e.g., printer). If an audit collection device is not attached, then it is necessary to purchase the audit reporting package from Spectrum in order to retrieve the audit data.

The DPS-800/12 system is independent of the host and cannot be tampered with by anyone who does not have access to the administrator's console. Only the system administrators may alter the parameters and database of users.

Once the user has been connected to the host, by the DPS-800/12, it will appear transparent to the user, except when entering the log off sequence.

The placement of the DPS-800/12 into a trusted computing environment must provide some assurances that it is performing it's function correctly. In order for such assurances to exist, the DPS-800/12 must be able to be installed and maintained in a secure manner, and the security relevant features must work properly.

Since the documentation is unclear and misleading, the system administrator may have a difficult time determining if the product has been properly installed and is operating in a secure manner. This is not to say that it cannot be operated in a secure manner. Only that, the system administrator may not be able to determine whether or not it is indeed doing so.

This page intentionally left blank

## Product Testing

### Test Procedure

Testing represents a significant portion of a subsystem evaluation. Unlike a system evaluation, design and implementation are not as closely examined as the functionality of the product. Subsystem testing must answer the question: Do the security features function correctly?

The test suite chosen by the team was designed to show if the system functionally meets those requirements. The first part of the test suite involved determining if the system administrator could properly control access to the system. The second part examined proper user identification and auditing of access attempts. The third part addressed what happened when a connection was broken.

All the tests were conducted using the DPS-800/12 configured with RS-232C asynchronous protocol cards. A microcomputer was used as the system administrator console and a line printer was used to capture the audit log. The terminals (microcomputers) were then attached to the host through the port cards. The cables used allowed the team to simulate the handshaking signals of a modem pair.

### Test Results

Testing of the product was carried out systematically to demonstrate the proper functioning of the security features of the product.

Tests regarding the system administrator functions demonstrated that most worked as described. The resource controls over port groups and time slots worked well; although the team did note that if a time slot expired while a user had access to the system, access was maintained until the user logs off. This is common in most systems.

Operation of the system showed that it properly controlled access to the host system. After the log on procedure, the DPS-800/12 appeared transparent to the user. However, testing of the log on procedure demonstrated the following:

> The user cannot change his own password. This is considered bad practice, as outlined in the *Password Management Guideline* (12 April 1985).
>
> The disconnect sequence could be a problem to users if they enter the sequence accidentally. Therefore, this should be a sequence which would not appear in a normal stream to the host computer (e.g. %%$$). Otherwise, the DPS-800/12 disconnects the user without warning. This is not stated in the *Operator Manual.*

In addition, the testing of the system administrator functions revealed the following:

The system did not prevent the installation of multiple passwords for the same UV-1, nor the same password for multiple UV-1's. Thus, the system did not enforce unique identification of users, unless the system administrator assigns unique passwords with unique time slots and/or port groups. This is not explained in the *Operator Manual* and should be.

If the audit device (printer) is not connected and online, audit records are lost and the system administrator is not informed of the fact. This contradicts the documentation, which states that these records are stored in an audit buffer on the printer control card.

The use of the "Lost UV-1" function produced undocumented results. When a UV-1, labeled as "lost", was used to access the system, its system identifier was nullified by a special control sequence. To reinstate a "Lost UV-1" a recovery function is used. However, testing showed that when recovery was attempted for a nullified UV-1 the password database was unexpectedly altered. Also, the UV-1 was not reinstated, because its system identifier was not corrected.